BAXTER

On the Complete Residue System of Certain Number Realms

Mathematics

A. M.

1912

ON THE COMPLETE RESIDUE SYSTEM OF CERTAIN NUMBER REALMS

BY

FLORENCE GABRIELLE BAXTER
A. B. University of Illinois, 1911

THESIS

Submitted in Partial Fulfillment of the Requirements for the

Degree of

MASTER OF ARTS

IN MATHEMATICS

IN

THE GRADUATE SCHOOL

OF THE

UNIVERSITY OF ILLINOIS

1912

UNIVERSITY OF ILLINOIS

THE GRADUATE SCHOOL

May 29 1912

I HEREBY RECOMMEND THAT THE THESIS PREPARED UNDER MY SUPERVISION BY

Miss Florence G. Baxter

ENTITLED On the complete residue system of certain number realms

BE ACCEPTED AS FULFILLING THIS PART OF THE REQUIREMENTS FOR THE

DEGREE OF A. M.

G. A. Miller

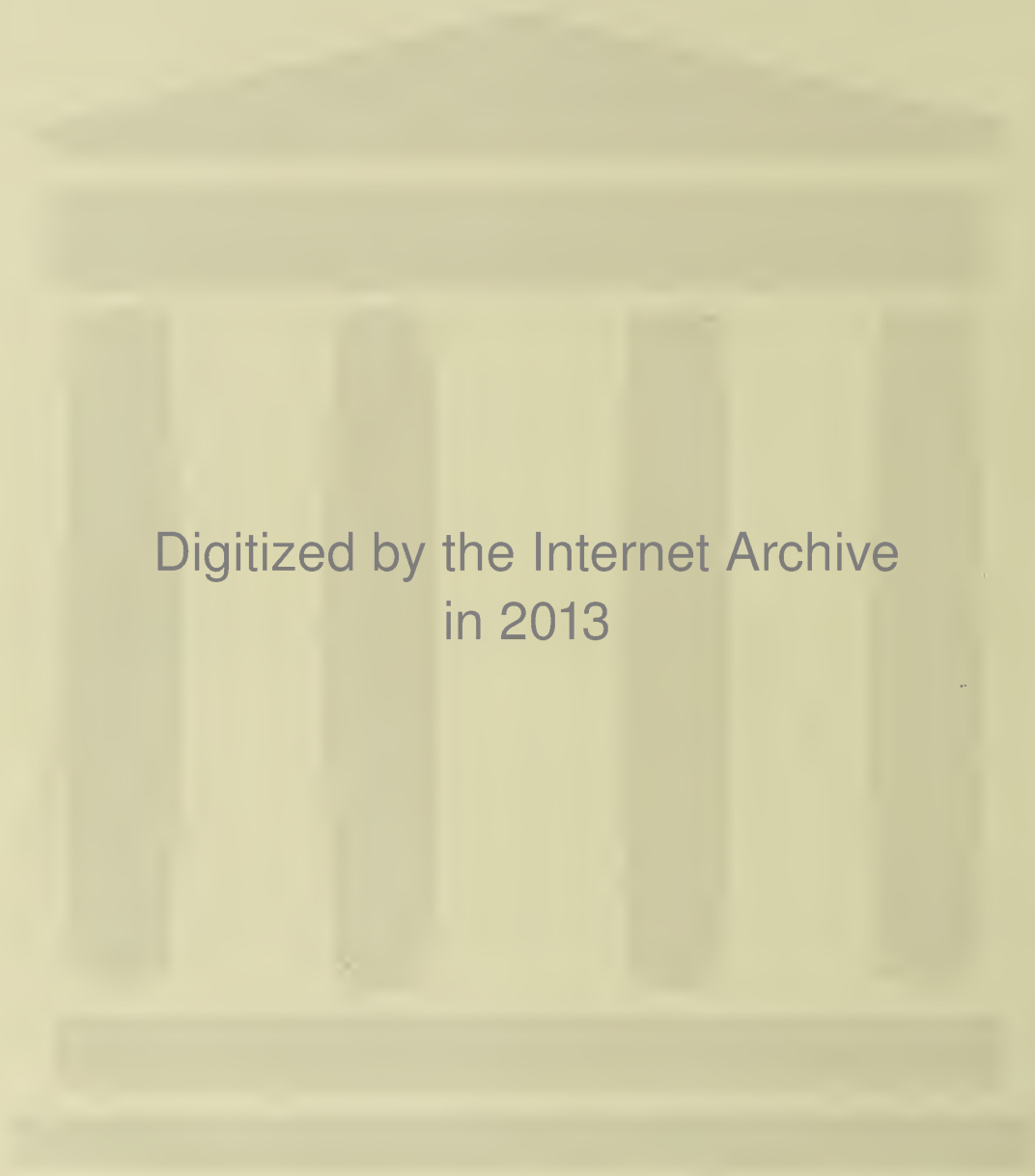
In Charge of Major Work

J. Townsend

Head of Department

Recommendation concurred in:

Committee on Final Examination



I N T R O D U C T I O N.

A new epoch in the theory of numbers dates from the publication of the Disquisitiones Arithmeticae, Leipzig, 1801. It was through this work that Gauss contributed to general mathematical literature the theory of congruences. In the preface to volume one he states that he had worked out the theory and was applying it in 1795. The term "congruence," however, was employed as early as 1730 by Goldbach (1) who, in one of his letters to Euler, used this nomenclature with the same meaning which Gauss applied to it later in the development of his theory. Goldbach's definition is stated as follows: "If a number $X=D\,P+R$ be given such that X is divisible by P with a remainder R, the remainder is called a 'numerum residuum', or, for the sake of brevity, a 'congruum.'" The following is a portion of the letter which he wrote to Euler (2) and in which the symbol $\perp\!\!\!\perp$ is used to express the incongruency:

$$"X^e \perp\!\!\!\perp P^m\chi + P \qquad (1)$$

where P is a prime integer, e and m denote integral positive numbers larger than one, and $\chi = \alpha + \beta x + \gamma x^2 + \cdots\cdots \lambda x^m$ with integral rational coefficients. Since $P^m\chi + P$ is divisible by P if (1) expresses a congruence X^e is divisible by P.

(1) Cantor, Geschichte der Mathematik Vol. III, 1901, p. 611.

(2) Corresp. Math. (Fuss). I. 25.
Commentorii Academiae Petropolitanae (1732-1733) T VI p. 103-107.

Then $X = AP$, $X^e = A^e P^e$ and we would have $A^e P^{e-1} = P^{m-1}\mathcal{K}+1$ which is impossible since $P \neq 1$."

The notion of congruences was extended by Gauss to apply to numbers of the realms K (i) and K $(\sqrt{-3})$. The matter is more clearly presented when it is expressed geometrically. In order to give a geometrical interpretation to certain concepts with regard to real numbers, a one to one correspondence has been assumed between the points on a line and the totality of real numbers. In the realms $K\sqrt{-M}$, where $\sqrt{-M}$ is an imaginary, a one to one correspondence has been established between the points of a plane and the totality of numbers in the realm. The first mathematician to propose a representation of the imaginary number $A\sqrt{-1}$ was Kühn of Danzig in 1750.(1) This was extended by Casper Wessel in a memoir of 1797(2) to include numbers of the form $A+B\sqrt{-1}$ where A and B are real numbers. However, the honor of this valuable extension has often been attributed to Argand, whose article did not appear until 1806, eight years after that of Casper Wessel, although it is probable Argand had never heard of the Norwegian surveyor, and knew nothing of his memoir. That the complex plane is known as the Argand plane is due to the fact that Wessel was not considered a mathematician, and that his theoretical work outside of the field of surveying was not scrutinized very closely, while the former's theory came to public knowledge by a controversy between Francais and Argand over a contribution which Francais sent to the "Annales de Gergonne" and which did not give due

(1) J. E. Cajori, Hist. of Math. (1901), p. 317.

(2) Beman, "Chapter on the Hist. of Math"., Proc. Amer. Assn. Adv. Science, (1897), p. 33-50.

credit to Legendre.[1] It was in the course of this discussion that the article of 1806 was republished. In spite of all of this publicity the contributions of Argand were passed by almost unnoticed. Hence when, about forty years later, representations of $A + B\,i$ were given independently by Warren of England and Mourey of France, their respective countries gave them all of the credit for their discovery. Wessel's memoir, "On the Analytic Representation of Direction" mentioned above, had for its object the determining of a method of expressing segments of straight lines by means of a unique equation between a single unknown segment and other given segments when we wish to find an expression representing at once the length and the direction of the unknown segment. He established the laws governing the addition, subtraction, multiplication and division of these segments, and showed these quantities to be of practical value in the demonstration of theorems, and in the solution of problems. His line segments are what have come to be known as vectors.

After the introduction of numbers of the form $A+B\,i$ some interesting theorems were soon added to the general theory. Among the most important of these is the fundamental theorem of algebra which was given its first rigorous proof by Gauss[2] in his thesis of 1797, and which was again demonstrated by Gauss in 1799 in his first published paper, "Demonstratio nova theorematis omnen functionem algebraicam rationalen integram imius variabilis in factores reales primis vel secundi gradus resolvi posse." It was in this

(1) M. J. Houel, "Argand les Quantities Imaginaires," 1874.

(2) Encyklopädie der Math. Wiss, 1900, p. 233.

article that Gauss mentioned the fact that he had a representation for imaginary quantities which he would later present. That occasion did not come until 1831, but in the meanwhile he gave three proofs of the fundamental theorem.[1] La Grange[2] worked for the most part in the approximation of roots, but the year following the appearance of Gauss' first proof he proved that every equation must have a root.

Analogous to the numbers of the form $A+B\,i$ of the realm $K(i)$ where A and B are rational integers are those of the form $A + B\rho$ of the realm $K\sqrt{-3}$ where ρ is a cube root of unity and A and B rational integers. The theory of these numbers proceeded from an attempt to solve problems of cubic reciprocity. The first results were published by Gauss in 1825 and were further extended by Jacobi in 1827, Dirichlet in 1842, and Eisenstein in 1844. When other quadratic realms were examined, it was found that in some realms the unique factorization theorem would not hold without the introduction of the concept of ideals. Kummer[3] introduced the ideal into the number reals in 1847. Following this, R. Dedekind and L. Kronecker gave the proof of the unique factorization of ideals in 1882.[4]

The integers of a general quadratic realm have been represented in a number of different ways. Klein supposes that the irreducible equation of the second degree is $AW^2 + 2\,B\,W + C$. The integers of the realm are given by the vertices of the system of parallelograms

(1) Comment. Götting 3, 1815, 1816. Götting, Abh. 4, 1850.
(2) La Grange, Resolutions des equations numerique, 1798.
(3) Crelle's Journal (1847), p. 319.
(4) Gött, Abh. 29. (1882); Crelle's Journal 92, (1882), p. 1.

whose sides are respectively $\sqrt{A}$ and $\sqrt{C}$ and the angle between them is arc. cos. $\frac{B}{\pm\sqrt{AC}}$. Minkowski and Klein have endeavored to represent geometrically in a more systematic fashion the results already known with regard to quadratic binaries, where the irreducible equation is $X^2 + M = 0$, M being a positive rational integer. By taking the axes 0 X and 0 Y and representing the system of values $X + Y\sqrt{-M}$ by the coördinates X, Y, the couples of numbers form a network of points. The unit of length is not supposed, however, to be the same on each of the axes. The network of points then constitute the corners of a network of parallelograms. Conversely any network of parallelograms represent the totality of couples of integers. Through the knowledge of three points (0, 0) (1, 0) (0, 1), called the base, the network is defined. Having given a network, the points are found which correspond to the couples of the numbers of the form

$$\alpha X + \beta Y$$
$$\gamma X + \delta Y$$

where $\alpha, \beta, \gamma, \delta$ are given integers and X, Y, variable integers. It is sufficient to find C (α, γ) and D (β, δ) to make the network of which 0 C D is the base.

In representing the integers of the realm K (i) Gauss used, in 1831, probably the siniplest method of representing the integers in the imaginary quadratic realms. The rectangular axes X and Y are taken as the axis of reals and the axis of imaginaries, respectively. The integers of the realm K $(i\sqrt{M})$ are $\frac{A+B\sqrt{-M}}{2}$ where A and B are both odd or both even in the case of $-M \equiv 1$, mod 4, and both even in the cases of $-M \equiv 2$ or 3, mod 4. $-M \equiv 0$ mod 4 is not considered since M is not supposed to contain any square

factor. The distance $A/_2$ is measured off along the axis of reals, and the distance $\frac{B\sqrt{M}}{2}$, along the axis of imaginaries. The coördinates $\left(\frac{A}{2}, \frac{B\sqrt{M}}{2}\right)$ then represent the integers of the realm.

One of the most important theorems coming out of the study of congruences is the law of quadratic reciprocity which Gauss calls the "gem" of higher arithmetic. Fermat (1) had known the quadratic character of -1 and at least partially that of 2 as early as 1640. In 1775 Lagrange investigated under what conditions ± 2 and ± 5 are quadratic residues or non residues of odd prime numbers. Euler discovered empirically the law of quadratic reciprocity for prime numbers, while Legendre (2) in 1785 worked out the first demonstration, complete at least for the case where not both P and Q are of the form $4H+1$. Gauss (3) proved the same theorem independently, in all giving ten proofs. The first proof which he gave, later simplified by G. Lejeune Dirichlet, is a demonstration by induction and applied to all numbers $P \equiv 1 \pmod 8$. Until the time of Jacobi the fourth section of the Disquisitiones Arithmetical treating of congruences of the second degree and the fifth section treating of quadratic forms were passed over with almost universal neglect. Jacobi found a law for the cubic residue based upon the law of quadratic reciprocity which Gauss published in a paper in 1831. It was in this paper that the terms "complex number" for $A+B\,i$ and "norm" for A^2+B^2 were used for the first time.

(1) Lettres de P de Fermat a Giles Personier, dit Roberval, aout 1640.

(2) A. M. Legendre, Hist. Acad. sc. Paris, 1785, M p. 513.

(3) Disq. Werke 1. p. 99/118.

The complete residue system with regard to a rational integer M as a modulus has been defined as the number of incongruent integers, mod M and is ~~equal to~~ composed of M integers.[1] In the realms K (i) and K ($\sqrt{-3}$)[2] the complete residue system (mod μ) is defined in the same way, and has been shown to ~~be equal to~~ be composed of $N_K(\mu)$ integers. When the integers of the quadratic realm are represented geometrically, the complete residue system may be contained in certain configurations in the plane. In the realm K (i) L. W. Reid[1] has suggested three theorems which lead to three different configurations. They will be found as theorems I, III and IV of the text.

The interpretation of the complete residue system has not been taken up as quickly as that of the reduced residue system. The latter consists, in any realm, of the incongruent integers, mod M prime to the modulus. The sign $\int(N)$ or $\int N$ for the number of integers of the reduced residue system of the rational realm is due to Euler[3], who at least understood its evaluation in 1760, but the notation $\phi(M)$ is due to Gauss who extended its use to the realm K (i). In a treatise on quadratic residues, 1831, he finds a general configuration which contains the reduced residue system, mod μ, where μ is an integer of the realm K (i).

(1) L. W. Reid, Elements of the Theory of Numbers, 1910, p. 182-185.

(2) Sommer, Vorlesungen uber Zahlentheorie, 1907.

(3) Commentat Arith. St. Petersb. 1849, p. 102.

(4) Disq. Arith. Leipzig, 1801.

CONFIGURATIONS CONTAINING THE COMPLETE RESIDUE SYSTEM.

The complete residue system in the three realms under consideration, $K(i)$, $K(\sqrt{-3})$ and the rational realm, may be given in an infinite number of ways. The following theorems give a manner of choosing the integers of the complete residue system with respect to certain moduli so that they may be contained exactly within a given figure.

Theorem I. If in the realm $K(i)$, $\mu = P + Q\,i$ where P and Q have no common divisor, the integers $1, 2, - - - - -, P^2 + Q^2 = N(\mu)$ form a complete residue system, mod μ.

All of the $N(\mu)$ integers $1, 2, - - - - -, P^2 + Q^2$ are incongruent, mod μ for $P^2 + Q^2$ is the smallest rational integer which $P + Q\,i$ divides. Suppose $P + Q\,i$ divides a smaller rational integer C, then

$$(P + Q\,I)\ (M - N\,I) = C < N(\mu). \qquad (1).$$

In order that this be possible we must have

$$M\,Q - N\,P = 0, \qquad (2).$$

$$\text{or} \qquad M = \frac{N\,P}{Q}, \quad N = \frac{M\,Q}{P} \qquad (3).$$

$$\text{and} \qquad C = M\,P + N\,Q < P^2 + Q^2 \qquad (4).$$

Substitute values of (3) in (4), then

$$C = \frac{n}{Q} \cdot P^2 + \frac{m}{P} \cdot Q^2 < P^2 + Q^2$$

Either $\frac{n}{Q} < 1$, $\frac{m}{P} < 1$ or both $\frac{N}{Q}$ and $\frac{M}{Q} < 1$ but since $P \neq Q$, $\frac{M}{Q}$ and $\frac{N}{Q}$ must be rational integers, which is impossible.

Since $P^2 + Q^2$ is the first rational integer which $P + Q\,I$ divides, all the integers 1 to $P^2 + Q^2$ inclusive are incongruent mod $P + Q\,I$. As these integers are norm (μ) in number, they form the complete residue system, mod μ and the theorem is proved.

Theorem II. If $\mu = P + Q\,I$, where P and Q have no common divisor, any norm (μ) consecutive integers form a complete residue system, where consecutive integers are those along any line parallel to the axis of reals at a distance 1 apart or along a line parallel to axis of imaginaries at distance i apart.

By Theorem I we know that the integers 1, 2, - - - - -, $P^2 + Q^2$ form a complete residue system. By adding to each integer the quantity $M + N\,i$, where M and N are any rational integral values, we obtain any N (μ) consecutive integers on the parallels to the X axis. Moreover, since in the first set the integers are incongruent, mod μ, the integers of the second set are incongruent, mod μ.

By multiplying the integers by i we obtain norm (μ) consecutive incongruent integers since i is a unit, but the set of integers are arranged parallel to the Y axis. Further-

more, if we add to each of these integers the quantity $M + N\,i$, where M and N are any rational integral values, we obtain any $N(\mu)$ consecutive, incongruent integers on the parallels to the Y axis. Hence the theorem is proven.

Theorem III. When $\mu = M\,(P + Q\,i)$ where P and Q have no common divisor and M is a rational integer, the complete residue system is contained within a rectangle consisting of the $M^2(P^2 + Q^2)$ integers

$$U + i\,V \begin{cases} U = 0,\ 1,\ - - - - -,\ M(P^2 + Q^2) - 1 \\ V = 0,\ 1,\ - - - - -,\ M - 1 \end{cases}$$

Now $M(P^2 + Q^2)$ is the rational integer of smallest absolute value divisible by μ which can be readily seen from Theorem I. From this it follows that the $M(P^2 + Q^2)$ integers along the x axis are incongruent, mod μ. Furthermore, no two of the $M(P^2 + Q^2)$ integers in each of the $M - 1$ rows above the X axis are congruent, mod μ. This follows directly from Theorem II. Also, no two integers of the M rows are congruent, mod μ. Suppose that $X + Y\,i = \alpha$ be any integer of the rectangle congruent to $U + i\,V = \beta$ any other integer of the rectangle.

Then $(X - U) + (Y - V)\,i \equiv 0$, mod $M(P\ \ Q\ I)$

whence $Y - V \equiv 0$, mod $M \cdot Q$.

But $Y - V < M$ so that for the above condition to hold $Y - V = 0$.

However, $X \not\equiv U$ mod $M(P + Q\,i)$

No two integers are congruent within the rectangle.

Theorem IV. If $\mu = M$, a rational integer, the complete residue, mod M is contained within and upon a square composed of the M integers

$$X+Y\,i \begin{cases} X = 0,\ 1,\ - - - - -,\ |M|-1 \\ Y = 0,\ 1,\ - - - - -,\ |M|-1 \end{cases}$$

This is a special case of Theorem III where $Q = 0$ and $P = 1$ and follows directly. It can be readily seen that both Theorems III and IV can be generalized to mean any rectangle of norm (μ) integers whose sides are respectively equal and parallel to the original rectangle.

Theorem V. When the modulus is of the form $\mu = M + (M+1)i$ where M is a positive rational integer, then the complete residue system, mod μ, is composed of the integers within and upon a square S, whose diagonals are situated on the X and Y axes respectively and are of length 2 M.

1. The square contains exactly norm (μ) integers.

If the integers of the complex plane be represented by the intersections of lines parallel to the X and Y axes respectively, every one of the integral points may be expressed in terms of its coördinates X and Y, where X and Y are rational entegral numbers. Let us consider the side of the square in the first quadrant expressed by the equation $X+Y = M$. As X is given the consecutive integral values 0, 1, 2, - - - - - M, Y takes the $M+1$ values M, $M-1$, - - - - -2, 1, 0. So that for the above equation X and Y have respectively $M+1$ pairs of integral

values, and therefore the number of integers, including the end points, on one side of the square is equal to $M+1$. As we take larger and larger squares by giving M the values 0, 1, 2, - - - - -, N we obtain, for the corresponding number of integers, an arithmetical progression.

The summation of this progression will give the number of integers within and upon the boundary of a quarter of the square. If we multiply this number by 4 the integers on the diagonals will all be repeated twice with the exception of the origin which will be repeated 4 times. If N = number of integers within and upon the sides of the square,

$$N = 4\,(1+2+3+\cdots\cdots+[m+1]) - 4m - 3$$

$$= 4\,(1+2+3+\cdots\cdots+[m+1]) - 4(m+1) + 1$$

$$= 4(1+2+3+\cdots\cdots+m) + 1$$

$$\sum_{m=1}^{m} m = \frac{m \cdot m+1}{2}$$

Then, $N = 4\left(\frac{m \cdot [m+1]}{2}\right) + 1$

But $n[\mu] = m^2 + (m+1)^2$

$$= 4\left(\frac{m \cdot [m+1]}{2}\right) + 1$$

$\therefore$ $N = \text{norm}\,[\mu]$.

2. No two integers within or upon the boundary of the Square are congruent, mod (μ).

Let $A+B\,i$ be any integer within or upon the square. Suppose that there is an integer $C+D\,i$ of the square congruent to $A+B\,i$, mod (μ). Since the equations of the four sides of the square may be expressed by the relation

$$X \pm Y = \pm M$$

we have since A and C are the X coördinates and B and D, the Y coördinates.

$$|A| + |B| \leq M \qquad (1).$$

$$|A| - |B| \leq M \qquad (2).$$

$$|C| + |D| \leq M \qquad (3).$$

$$|C| - |D| \leq M \qquad (4).$$

If $A+B\,i$ and $C+D\,i$ are congruent, mod (μ).

$$(A+B\,i) - (C+D\,i) = K\ (M+(M+1)\,i).$$

$$(A-C)^2 + (B-D)^2 = (\text{norm } K)(2M^2+2M+1)$$

$$A^2-2AC+C^2+B^2-2BD+D^2=(\text{norm } K)(2M^2+2M+1). \qquad (6)$$

Squaring (1) and (2) and adding and likewise (3) and (4) we have,

$$A^2+B^2 \leq M^2 \qquad (7)$$

$$C^2+D^2 \leq M^2 \qquad (8)$$

Multiplying (1) and (3), (2) and (4) and adding we have

$$2\,|AC| \quad 2\,|BD| \leq 2M^2 \qquad (9)$$

Substituting (7) (8) and (9) in (6) we have

$$(2M^2+2M+1)\ \text{norm } K \leq 4M^2 \qquad (10)$$

We have three cases to consider, namely: (norm K) $\geq$ 2 or (norm K) = 1. It can be readily seen from (10) (norm K) $\neq$ 2 otherwise $4M^2 + 4M + 2 \leq 4M$ or $K \leq 4M^2$ where $K > 4M^2 + 4M + 2$. This is impossible since M is always positive.

If norm K = 1. and $A + BI \equiv C + DI \mod (\mu)$.

$(A + BI) - (C + DI) = M + (M + 1)i$

Equating real and imaginary parts

$A - C = M \qquad B - D = M + 1$

Since A, B, C or D is not $> M$. The condition for congruency is

$$|A| + |C| = M \qquad |B| + |D| = M + 1$$

Adding

$|A| + |B| + |C| + |D| = 2M + 1$ which is impossible since from equation (1) and (2)

$|A| + |B| + |C| + |D| \leq 2M$

. . Since $A + BI$ and $C + DI$ were taken as any two integers within or upon the square then no two integers of the square are congruent, mod (μ)

Hence the theorem follows.